IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s): B.M. Jakobsson et al.
Case: EMC-06-463
Serial No.: 10/631,989
Filing Date: July 31, 2003
Group: 2437
Examiner: Tamara Teslovich

Title: Method and Apparatus for Graph-Based Partition of Cryptographic Functionality

---

APPEAL BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

Applicants (hereinafter "Appellants") hereby appeal the final rejection dated December 9, 2008 of claims 1-30 of the above-identified application.

REAL PARTY IN INTEREST

The real party in interest is RSA Security Inc., the assignee of record, which is a subsidiary of EMC Corporation.

RELATED APPEALS AND INTERFERENCES

There are no known related appeals and interferences.

STATUS OF CLAIMS

The present application was filed on July 31, 2003 with claims 1-30, all of which remain pending. Claims 1 and 28-30 are the independent claims.

Claims 1-30 are rejected under 35 U.S.C. §112, second paragraph, and under 35 U.S.C. §102(e).

Claims 1-30 are appealed.

STATUS OF AMENDMENTS

There have no amendments filed subsequent to the final Office Action.

SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 is directed to a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The method includes the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level. The transmitted information includes the first seed but not the second seed.

As described in the specification at, for example, page 6, lines 6-25, an illustrative embodiment includes a method (e.g., 300 in FIG. 3) for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device (e.g., 102D in FIG. 1) to at least one recipient device (e.g., 104R in FIG. 1). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page

6, lines 19-21, the method includes the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 28 is directed to an apparatus comprising a processing device comprising a processor coupled to a memory. The processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The processing device is configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 22, to page 6, line 5, an apparatus (e.g., 102D in FIG. 1) comprises a processing device comprising a processor (e.g., 200 in FIG. 2) coupled to a memory (e.g., 202 in FIG. 2). As described in the specification at, for example, page 4, lines 24-26, and page 6, lines 6-25, the processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device (e.g., 102D in FIG. 1), to at least one recipient device (e.g., 104R in FIG. 1). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page 6, lines 19-21, the processing device is configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 29 is directed to an apparatus comprising a processing device comprising a processor coupled to a memory. The processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least

one delegating device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes, and a given set of the nodes is associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality. The processing device is operative to receive from the delegating device information representative of one or more of the nodes, and the processing device is configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the received information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 22, to page 6, line 5, an apparatus (e.g., 102R in FIG. 1) comprises a processing device comprising a processor (e.g., 200 in FIG. 2) coupled to a memory (e.g., 202 in FIG. 2). As described in the specification at, for example, page 6, lines 6-25, the processing device is utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device (e.g., 102R), from at least one delegating device (e.g., 102D). As described in the specification at, for example, page 6, lines 26-28, the cryptographic functionality is characterized as a graph comprising a plurality of nodes, such as the exemplary graphs shown in FIGS. 5-9 and described in the specification at, for example, page 13, line 3, to page 14, line 14, and a given set of the nodes is associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 19-25, with reference to step 302 in FIG. 3, the processing device is operative to receive from the delegating device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the processing device is configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each

level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

Claim 30 is directed to a machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. The cryptographic functionality is characterized as a graph comprising a plurality of nodes. The one or more software programs, when executed by the delegating device, implement the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. The recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. The nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. A first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

In an illustrative embodiment described in the specification at, for example, page 5, line 28, to page 6, line 12, a machine-readable storage medium (e.g., memory 202 in FIG. 2) contains one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device (e.g., 102D in FIG. 1) to at least one recipient device (e.g., 102R in FIG. 1), wherein the cryptographic functionality is characterized as a graph comprising a plurality of nodes. As described in the specification at, for example, page 6, lines 12-16, and with reference to step 302 in FIG. 3 at page 6, lines 19-21, the one or more software programs, when executed by the delegating device, implement the steps of associating a given set of the nodes with a corresponding one of the plurality of distinct

portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes. As described in the specification at, for example, page 6, lines 21-25, with reference to step 304 in FIG. 3, the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. As described in the specification at, for example, page 6, lines 17-18, the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, and the nodes correspond to respective seeds. As discussed in the specification at, for example, page 7, line 9, to page 9, line 14, with reference to FIG. 4, and page 16, lines 18-25, a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and the transmitted information includes the first seed but not the second seed.

As described in the specification at, for example, page 3, lines 10-15; page 15, lines 16-25; page 17, lines 21-26; and page 25, lines 1-28, illustrative embodiments of the present invention provide a number of advantages relative to conventional techniques. For example, an illustrative embodiment may permit delegation on a per-computation rather than per-interval basis, and thus do not require a third party to know the particular intervals or segments into which computational ability has been partitioned, nor do they require a separate transmission for each interval. Another important advantage is that an illustrative embodiment may provide a particularly efficient mechanism for the provision of cryptographic functionality in accordance with a subscription model.

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-30 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite.

2. Claims 1-30 are rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Application Publication No. 2007/0226807 (hereinafter "Ginter").

ARGUMENT

1. Rejection of claims 1-30 under 35 U.S.C. §112, second paragraph

Appellants initially note that the test for definiteness under §112, second paragraph, is whether "those skilled in the art would understand what is claimed when the claim is read in light of the specification." *Orthokinetics, Inc. v. Safety Travel Chairs, Inc.*, 806 F.2d 1565, 1576, 1 USPQ2d 1081, 1088 (Fed. Cir. 1986). A rejection under §112, second paragraph, for indefiniteness is only appropriate if the language of the claim is such that a person of ordinary skill in the art could not interpret the metes and bounds of the claim so as to understand how to avoid infringement. See *Metabolite Labs., Inc. v. Lab. Corp. of Am. Holdings*, 370 F.3d 1354, 1366, 71 USPQ2d 1081, 1089 (Fed. Cir. 2004) ("The requirement to 'distinctly' claim means that the claim must have a meaning discernible to one of ordinary skill in the art when construed according to correct principles. . . . Only when a claim remains insolubly ambiguous without a discernible meaning after all reasonable attempts at construction must a court declare it indefinite.")

In formulating the rejection under §112, second paragraph, in the Office Action at page 6, last paragraph, the Examiner argues that the language recited in claim 1 "fails to provide the necessary structural relationship between these seeds and his [sic] underlying system." Appellants respectfully disagree and instead submit that claim 1 does in fact describe the manner in which the limitations regarding seeds are related to the other limitations.

More particularly, claim 1 is directed to a method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device. This method includes a step of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality. Claim 1 specifies that the cryptographic functionality is characterized as a graph comprising a plurality of nodes, and that the nodes correspond to respective seeds.

The method recited in claim 1 also includes a step of transmitting from the delegating device to the recipient device information representative of one or more of the nodes, and specifies that the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality. Claim 1

specifies that the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, that a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and that the transmitted information includes the first seed but not the second seed.

Claims 28-30 contain language similar to that discussed above with reference to claim 1, and therefore believed to be similarly definite.

The Examiner further alleges that it is unclear what the relationship is between the "respective seeds" recited in claim 1 and the limitation of dependent claim 22 wherein the recited cryptographic functionality comprises an ability to compute one or more seeds.

Claim 1 specifies that the cryptographic functionality is characterized as a graph comprising a plurality of nodes, and that the nodes correspond to respective seeds. More particularly, claim 1 specifies that the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level, that a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level. Claim 1 specifies that the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality, and that the transmitted information includes the first seed but not the second seed.

Appellants respectfully submit that dependent claim 22 is directed to an embodiment wherein the recited cryptographic functionality comprises an ability to compute one or more seeds. As is clear from the specification at page 14, lines 6-14, with reference to FIG. 9, the one or more seeds recited in claim 22 could be, but need not be, associated with nodes included within the same graph as the respective seeds recited in claim 1. In other words, the respective seeds recited in claim 1 could, but need not, include the one or more seeds recited in claim 22.

Appellants respectfully note that "[b]readth of a claim is not to be equated with indefiniteness." See MPEP 2173.04 (citing *In re Miller*, 441 F.2d 689, 169 USPQ 597 (CCPA 1971)). See, e.g., *Ex parte Nolden*, 149 USPQ 378, 380 (Bd. Pat. App. 1965) ("[I]t is not essential to a patentable combination that there be interdependency between the elements of the claimed device or that all the elements operate concurrently toward the desired result"); *Ex parte Huber,* 148 USPQ 447, 448-49 (Bd.

Pat. App. 1965) (A claim does not necessarily fail to comply with 35 U.S.C. 112, second paragraph where the various elements do not function simultaneously, are not directly functionally related, do not directly intercooperate, and/or serve independent purposes.)

Accordingly, Appellants respectfully assert that the claims at issue comply with §112, second paragraph.

2. Rejection of claims 1-30 under §102(e) over Ginter

Claims 1-8, 17-21 and 24-30

With regard the §102(e) rejection of claims 1-30, Appellants initially note that the Federal Circuit has recently reiterated that "unless a reference discloses within the four corners of the document not only all of the limitations claimed but also all of the limitations arranged or combined in the same way as recited in the claim, it cannot be said to prove prior invention of the thing claimed and, thus, cannot anticipate under 35 U.S.C. §102." *Net MoneyIN Inc. v. VeriSign Inc.*, 545 F.3d 1359, 1369, 88 USPQ2d 1751, 1760 (Fed. Cir. 2008)

The Examiner argues that the Ginter reference teaches each and every one of the limitations of claim 1. Appellants respectfully disagree. For example, claim 1 recites limitations wherein the recited method includes steps of associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and transmitting from the delegating device to the recipient device information representative of one or more of the nodes.

In formulating the rejection of claim 1, the Examiner relies on paragraphs 73, 74, 92, 110 and 112 of Ginter as allegedly teaching the recited associating and transmitting steps. See the Office Action at page 7, last paragraph, through page 8, second paragraph. However, these relied-upon portions of Ginter fail to teach or suggest the association of particular nodes of a graph with one of a number of distinct portions of partitioned cryptographic functionality, and further fail to teach or suggest the transmission of information representative of one or more of such nodes from a delegating device to a recipient device so as to configure the recipient device for authorized execution of a portion of the partitioned cryptographic functionality. To the contrary, these portions of Ginter primarily discuss in

very general terms various aspects of a virtual distribution environment or VDE. The particular recitations at issue are clearly not met by these general teachings from Ginter.

Moreover, claim 1 includes further limitations wherein the nodes correspond to respective seeds, wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and wherein the transmitted information includes the first seed but not the second seed.

In arguing that Ginter meets these limitations of claim 1, the Examiner relies primarily on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 8, fifth and sixth paragraphs. Appellants respectfully submit that the relied-upon portions of Ginter contain no disclosure of any technique wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level, and wherein the transmitted information includes the first seed but not the seed.

Paragraphs 1519 and 1521 of Ginter teach directly away from the claimed technique by describing arrangements in which each seed is randomly generated, and hence is independent of one another. Paragraph 1452 of Ginter suggests that each of these seeds may be used to generate a corresponding key which may used to decrypt a corresponding portion of a content object. However, these is simply no disclosure of any technique wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level. See Ginter at paragraph 1452:

> For security purposes, a content object may be encrypted with more than one key. For example, a movie may have the first 10 minutes encrypted using a first key, the second 10 minutes encrypted with a second key, and so on. These keys are stored in a PERC 808 in a structure called a "key block." The selection process involves determining the correct key to use from the key block in order to decrypt the content. . . . DECRYPT method 2030 may then access an appropriate PERC 808 from the secure database 610 and loads a key (or "seed") from a PERC (blocks 2034, 2036). This key information may be the actual decryption key to be used to decrypt the content, or it may be information from which the decryption key may be at least in part derived or calculated. If necessary, DECRYPT method 2030 computes the decryption key based on the information read from PERC 808 at block 2034 (block 2038). DECRYPT method 2030 then uses the obtained and/or calculated decryption key to actually decrypt the block of encrypted information (block 2040). DECRYPT method 2030 outputs the decrypted

block (or the pointer indicating where it may be found), and terminates (termination point 2042).

Accordingly, it is believed that Ginter fails to meet the limitations of independent claim 1.

Claims 2-8, 17-21 and 24-27 are believed allowable at least by virtue of their dependency from independent claim 1.

Independent claims 28-30 are believed allowable for reasons similar to those outlined above with regard to claim 1.

Claim 9

In addition to being allowable at least by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 9 is believed to define additional separately-patentable subject matter. More particularly, dependent claim 9 includes a limitation wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node.

In formulating the rejection of claim 9, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 10, second paragraph. Appellants respectfully submit that the relied-upon portions of Ginter fail to disclose any arrangement in which a graph comprises levels of nodes, wherein a level comprises a parent node and a set of seeds each derivable from the parent node. As noted above with reference to claim 1, there is simply no disclosure within Ginter of a technique in which one seed is derivable from another seed. Thus, Ginter clearly fails to disclose a technique in which a level of nodes comprises a parent node and a set of seeds each derivable from the parent node, as recited in claim 9.

Claim 10

Claim 10 is allowable at least by virtue of its dependency from independent claim 1 and dependent claim 9, each of which is believed to be separately patentable for the reasons discussed above. Claim 10 is also believed to define additional separately-patentable subject matter. More

particularly, dependent claim 10 includes a limitation wherein an *i*th node of a *k*th one of the levels is computed as $f_k(i, v_{k+1})$, where f_k is a one-way function.

In formulating the rejection of claim 10, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 10, third paragraph. As noted above with reference to claim 1, there is simply no disclosure within Ginter of a technique in which one seed is computed as a function of another seed. Thus, Ginter clearly fails to disclose a technique in which a node of one of the levels is computed as a function of a seed within another level, as recited in claim 10.

Claim 11

Claim 11 is allowable at least by virtue of its dependency from independent claim 1 and dependent claims 9 and 10, each of which is believed to be separately patentable for the reasons discussed above. Claim 11 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 11 includes a limitation wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

In formulating the rejection of claim 11, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 10, fourth paragraph. Appellants respectfully submit that there is no teaching within the relied-upon portions of Ginter of any technique in which nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

Claim 12

Claim 12 is allowable at least by virtue of its dependency from independent claim 1 and dependent claims 9-11, each of which is believed to be separately patentable for the reasons discussed above. Claim 12 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 12 includes a limitation wherein the *i*th node of a *j*th tuple of the *k*th level is computed as $f_k(j, i, v_{k+1,j})$.

In formulating the rejection of claim 12, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 10, fifth paragraph. As noted above with reference to claim 1, there is simply no disclosure within Ginter of a technique in which one seed is computed as

a function of another seed. Thus, as noted above with reference to claim 10, Ginter clearly fails to disclose a technique in which a node of one of the levels is computed as a function of a seed within another level, as recited in claim 12.

Claim 13

In addition to being allowable at least by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 13 is believed to define additional separately-patentable subject matter. More particularly, claim 13 includes a limitation wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token. Appellants note that claim 1, the limitations of which are incorporated into claim 13 under 35 U.S.C. §112, fourth paragraph, specifies that the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

In formulating the rejection of claim 13, the Examiner relies on Ginter at paragraphs 74, 1114 and 2187. See the Office Action at page 11, first paragraph. Paragraph 74 of Ginter states, in very general terms, that "VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), with other technologies including: . . . smart card, and semiconductor design technologies."

Paragraph 1114 of Ginter states that "[i]nitiation of load module execution in this environment is strictly controlled by a combination of access tags, encryption keys, digital signatures and/or correlation tags." Paragraph 2187 of Ginter generally states that "there is increased discussion concerning the distribution of content across networks. . . ."

Appellants respectfully submit that there is no teaching within the cited portions of Ginter, or elsewhere within Ginter, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises a cryptographic functionality provided by a hardware-based authentication token. For example, there is no disclosure of a technique in which a recipient device is configured based on the transmitted information for authorized execution of a

corresponding one of the plurality of distinct portions of a cryptographic functionality comprising a cryptographic functionality provided by a hardware-based authentication token.

Claim 14

In addition to being allowable at least by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 14 is believed to define additional separately-patentable subject matter. More particularly, claim 14 includes a limitation wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token. Appellants note that claim 1, the limitations of which are incorporated into claim 14 under 35 U.S.C. §112, fourth paragraph, specifies that the recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

In formulating the rejection of claim 14, the Examiner relies on Ginter at paragraphs 74, 1114 and 2187. See the Office Action at page 11, second paragraph. Paragraph 74 of Ginter states, in very general terms, that "VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), with other technologies including: . . . smart card, and semiconductor design technologies."

Paragraph 1114 of Ginter states that "[i]nitiation of load module execution in this environment is strictly controlled by a combination of access tags, encryption keys, digital signatures and/or correlation tags." Paragraph 2187 of Ginter generally states that "there is increased discussion concerning the distribution of content across networks. . . ."

Appellants respectfully submit that there is no teaching within the cited portions of Ginter, or elsewhere within Ginter, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token. For example, there is no disclosure of a technique in which a recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct

portions of a cryptographic functionality comprising an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

Claim 15

Claim 15 is allowable at least by virtue of its dependency from independent claim 1 and dependent claim 14, each of which is believed to be separately patentable for the reasons discussed above. Claim 15 is also believed to define additional separately-patentable subject matter. More particularly, dependent claim 15 includes a limitation wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

In formulating the rejection of claim 15, the Examiner relies on Ginter at paragraphs 510 and 1452. See the Office Action at page 11, third paragraph. Paragraph 510 of Ginter states that "random number generator 542 may provide specialized hardware circuitry for generating random values. . . . Such random values may are particularly useful for constructing encryption keys. . . . A random number of arbitrary size may be constructed by concatenating values produced by random number generator 542." As noted above with reference to claim 1, paragraph 1452 of Ginter suggests that each of a plurality of seeds generated by such a random number generator may be used to generate a corresponding key which may used to decrypt a corresponding portion of a content object. However, there is no disclosure of a verification operation performed collaboratively by at least first and second servers each storing one of the seeds, as recited in claim 15.

Claim 16

In addition to being allowable at least by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 16 is believed to define additional separately-patentable subject matter. More particularly, claim 16 includes a limitation wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token. Appellants note that claim 1, the limitations of which are incorporated into claim 16 under 35 U.S.C. §112, fourth paragraph, specifies that the

recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

In formulating the rejection of claim 16, the Examiner relies on Ginter at paragraphs 74, 1114 and 2187. See the Office Action at page 11, fourth paragraph. Paragraph 74 of Ginter states, in very general terms, that "VDE normally employs an integration of cryptographic and other security technologies (e.g. encryption, digital signatures, etc.), with other technologies including: . . . smart card, and semiconductor design technologies."

Paragraph 1114 of Ginter states that "[i]nitiation of load module execution in this environment is strictly controlled by a combination of access tags, encryption keys, digital signatures and/or correlation tags." Paragraph 2187 of Ginter generally states that "there is increased discussion concerning the distribution of content across networks. . . ."

Appellants respectfully submit that there is no teaching within the cited portions of Ginter, or elsewhere within Ginter, which meets the limitations at issue, which specify that a technique in which the cryptographic functionality recited in claim 1 comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token. For example, there is no disclosure of a technique in which a recipient device is configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of a cryptographic functionality comprising an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

Claim 22

In addition to being allowable at least by virtue of its dependency from independent claim 1, the patentability of which is discussed above, claim 22 is believed to define additional separately-patentable subject matter. More particularly, dependent claim 22 includes a limitation wherein the cryptographic functionality comprises an ability to compute one or more seeds. Appellants note that claim 1, the limitations of which are incorporated into claim 22 under 35 U.S.C. §112, fourth paragraph, specifies that the recipient device is configured based on the transmitted information for authorized

execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality.

In formulating the rejection of claim 22, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 22, fifth paragraph. Appellants respectfully submit that the relied-upon portions of Ginter fail to disclose any arrangement in which a recipient device is configured based on transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of a cryptographic functionality comprising an ability to compute one or more seeds.

Rather, as noted above with reference to claim 1, paragraphs 1519 and 1521 of Ginter teach directly away from the claimed technique by describing arrangements in which each seed is randomly generated in an independent manner. Paragraph 1452 of Ginter suggests that each of these seeds may be used to generate a corresponding key which may used to decrypt a corresponding portion of a content object. There is simply no disclosure of configuring a recipient device, based on transmitted information, for authorized execution of a corresponding one of the plurality of distinct portions of a cryptographic functionality comprising an ability to compute one or more seeds, as recited in claim 22.

Claim 23

Claim 23 is allowable at least by virtue of its dependency from independent claim 1 and dependent claim 22, each of which is believed to be separately patentable for the reasons discussed above. Claim 23 is also believed to define additional separately-patentable subject matter. More particularly, claim 23 includes a limitation wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

In formulating the rejection of claim 23, the Examiner again relies on Ginter at paragraphs 610, 1452, 1519 and 1521. See the Office Action at page 22, sixth paragraph. Appellants respectfully submit that the relied-upon portions of Ginter fail to disclose any arrangement in which a recipient device is configured based on transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of a cryptographic functionality comprising an ability to compute

one or more seeds, as recited in claim 22, much less the further limitation of claim 23 wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

In view of the above, Appellants believe that claims 1-30 are in condition for allowance, and respectfully request reversal of the present rejections.

Respectfully submitted,

Date: April 13, 2009

Joseph B. Ryan
Attorney for Applicant(s)
Reg. No. 37,922
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-7517

CLAIMS APPENDIX

1. A method for partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, the method comprising the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

2. The method of claim 1 wherein at least one of the nodes of the graph corresponds to a seed the possession of which permits execution of a corresponding one of the distinct portions of the cryptographic functionality.

3. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least two of the nodes.

4. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one parent node of the graph.

5. The method of claim 1 wherein the transmitting step further comprises transmitting from the delegating device to the recipient device information representative of at least one child node of a parent node of the graph.

6. The method of claim 1 wherein the graph comprises at least first and second root nodes.

7. The method of claim 1 wherein the graph comprises a tree having at least first and second subtrees associated with respective first and second ones of the plurality of distinct portions of the cryptographic functionality.

8. The method of claim 1 wherein the graph comprises a chain.

9. The method of claim 1 wherein the graph comprises L levels of nodes, an Lth one of the levels comprising a parent node $v_{L,1}$, and a first one of these levels comprising a set of seeds $v_{1,1}, v_{1,2}, \ldots v_{1,n}$, where n is the total number of seeds, each of the seeds being derivable from the parent node.

10. The method of claim 9 wherein an ith node of a kth one of the levels is computed as $f_k(i, v_{k+1})$, where f_k is a one-way function.

11. The method of claim 10 wherein the nodes of one or more of the levels are arranged in the form of tuples of designated numbers of nodes.

12. The method of claim 11 wherein the ith node of a jth tuple of the kth level is computed as $f_k(j, i, v_{k+1,j})$.

13. The method of claim 1 wherein the cryptographic functionality comprises a cryptographic functionality provided by a hardware-based authentication token.

14. The method of claim 1 wherein the cryptographic functionality comprises an ability to verify at least one of an authentication code and a distress code generated by a hardware-based authentication token.

15. The method of claim 14 wherein the authentication token is configured to store at least two seeds, and the cryptographic functionality comprises a verification operation performed collaboratively by at least first and second servers each storing one of the seeds.

16. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate at least one of an authentication code and a distress code utilizing a hardware-based authentication token.

17. The method of claim 1 wherein the cryptographic functionality comprises at least one of an ability to verify a signature and an ability to generate a signature.

18. The method of claim 1 wherein the cryptographic functionality comprises an ability to generate one or more values of a one-way chain.

19. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform symmetric cryptographic operations.

20. The method of claim 1 wherein the cryptographic functionality comprises an ability to perform asymmetric cryptographic operations.

21. The method of claim 1 wherein the cryptographic functionality comprises an ability to derive one or more cryptographic keys.

22. The method of claim 1 wherein the cryptographic functionality comprises an ability to compute one or more seeds.

23. The method of claim 22 wherein at least one of the seeds corresponds to at least one of the nodes of the graph.

24. The method of claim 1 wherein the cryptographic functionality is partitioned in accordance with a subscription model which requires compliance with at least one specified criterion for transmission from the delegating device to the recipient device of the information representative of one or more of the nodes.

25. The method of claim 24 wherein compliance with the specified criterion is satisfied upon receipt of a designated payment.

26. The method of claim 1 wherein the recipient device and the delegating device collaborate to perform at least one of a cryptographic verification function and a cryptographic generation function.

27. The method of claim 26 wherein the recipient device includes only a limited computational ability associated with performance of the cryptographic function.

28. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from the processing device, configured as a delegating device, to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

the processing device being configured to associate a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality, and to transmit to the recipient device information representative of one or more of the nodes, the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

29. An apparatus comprising:

a processing device comprising a processor coupled to a memory;

the processing device being utilized in conjunction with partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality to the processing device, configured as a recipient device, from at least one delegating device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes;

a given set of the nodes being associated with a corresponding one of the plurality of distinct portions of the cryptographic functionality;

the processing device being operative to receive from the delegating device information representative of one or more of the nodes, the processing device being configured based on the received information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the received information including the first seed but not the second seed.

30. A machine-readable storage medium containing one or more software programs for use in partitioning of cryptographic functionality so as to permit delegation of at least one of a plurality of distinct portions of the cryptographic functionality from a delegating device to at least one recipient device, the cryptographic functionality being characterized as a graph comprising a plurality of nodes, wherein the one or more software programs when executed by the delegating device implement the steps of:

associating a given set of the nodes with a corresponding one of the plurality of distinct portions of the cryptographic functionality; and

transmitting from the delegating device to the recipient device information representative of one or more of the nodes;

the recipient device being configured based on the transmitted information for authorized execution of a corresponding one of the plurality of distinct portions of the cryptographic functionality;

wherein the nodes of the graph are arranged in a plurality of levels with one or more nodes at each level;

wherein the nodes correspond to respective seeds; and

wherein a first seed associated with a node of a first one of the levels is computed as a function of a second seed associated with a node of a second one of the levels higher than the first level;

the transmitted information including the first seed but not the second seed.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.